PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-175403
(43)Date of publication of application : 02.07.1999

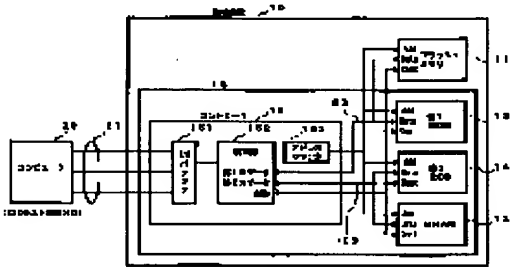
(51)Int.Cl. G06F 12/14
G06F 12/16
G11C 16/02
G11C 29/00

(21)Application number : 09-335614
(22)Date of filing : 05.12.1997

(71)Applicant : TOKYO ELECTRON LTD
(72)Inventor : NAKAMURA YASUHIRO

(54) TEST METHOD FOR STORAGE DEVICE AND MEMORY PROVIDED WITH TEST FUNCTION

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a test method for testing a storage area storing a decoding program without leaking an enciphered cryptographic key to the outside in a storage device for enciphering and storing data.
SOLUTION: An enciphered cryptographic key (k) is stored in a flash memory 11. A decoding program for decoding the cryptographic key (k) is stored in a ROM 14 where the access from the outside is inhibited and protected. The cryptographic key(k) is decoded by the decoding program, data are enciphered by using the cryptographic key (k) to store the data in the flash memory 11 and the data read from the flash memory 11 are decoded by the cryptographic key (k) to be outputted. The data constituting the decoding program are processed by a hash function stored in the ROM 14 for checking an area for storing the decoding program, the processed result is compared with an expected value and when they are coincident, it is judged that the storage area is normal.



LEGAL STATUS
[Date of request for examination] 03.10.2000
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－175403

(43)公開日　平成11年(1999)７月２日

(51)Int.Cl.[6]		識別記号	FI		
Ｇ０６Ｆ	12/14	３２０	Ｇ０６Ｆ	12/14	３２０Ａ
	12/16	３３０		12/16	３３０Ａ
Ｇ１１Ｃ	16/02		Ｇ１１Ｃ	29/00	６７１Ｚ
	29/00	６７１		17/00	６０１Ａ

審査請求　未請求　請求項の数13　ＯＬ　（全 11 頁）

(21)出願番号　特願平9－335614

(22)出願日　平成９年(1997)12月５日

(71)出願人　000219967
東京エレクトロン株式会社
東京都港区赤坂５丁目３番６号

(72)発明者　中村　泰弘
東京都府中市住吉町２丁目30番地の７　東京エレクトロン株式会社府中事業所内

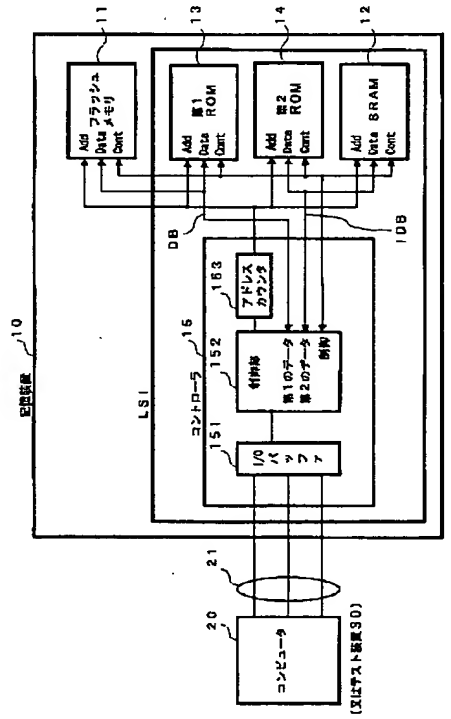
(74)代理人　弁理士　木村　満　（外３名）

(54)【発明の名称】　テスト機能を備える記憶装置及びメモリのテスト方法

(57)【要約】

【課題】　データを暗号化して記憶する記憶装置において、暗号化された暗号鍵の復号プログラムを外部に漏らすことなく、かつ、復号プログラムを記憶エリアのテストを可能とするテスト方法を提供する。

【解決手段】　フラッシュメモリ１１には、暗号化された暗号鍵ｋが記憶されている。外部からのアクセスが禁止されて、プロテクトされたＲＯＭ１４には、暗号鍵ｋを復号するための復号プログラムが記憶されている。この復号プログラムで暗号鍵ｋを復号し、この暗号鍵ｋを用いてデータを暗号化してフラッシュメモリ１１に格納し、フラッシュメモリ１１から読み出したデータを暗号鍵ｋで復号して出力する。復号プログラムを格納したエリアをチェックするため、復号プログラムを構成するデータをＲＯＭ１４に格納されたハッシュ関数で処理し、処理結果と期待値とを比較し、一致するとき、正常であると判別する。



1

【特許請求の範囲】

【請求項１】データを記憶するための第１の記憶手段（フラッシュ１１）と、

暗号鍵が暗号化されて記憶されている第２の記憶手段（フラッシュ１１）と、

前記暗号鍵（ｋ）を復号化するための復号情報が格納された第３の記憶手段（Ｔ２）と、

前記第３の記憶手段をテストするための関数を記憶した第４の記憶手段（Ｔ４）と、

前記第３の記憶手段に記憶された復号情報を用いて前記暗号鍵を復号化し、外部より供給されるデータを復号化した暗号化鍵を用いて暗号化して、前記第１の記憶手段に書き込む書込手段（１５）と、

前記第３の記憶手段に記憶された復号情報を用いて前記暗号鍵を復号化し、復号化された暗号鍵を用いて前記第１の記憶手段から読み出されたデータを復号化して出力する読出手段（１５）と、

前記第３の記憶手段に記憶された復号情報を前記第４の記憶手段に記憶された関数で処理し、得られた値と期待値を比較し、比較結果を出力する比較手段と（１５）、を備えることを特徴とする記憶装置。

【請求項２】前記第１、第２、及び第４の記憶手段の少なくとも１つの記憶手段のアドレスをスキャンして、その記憶内容を読み出すことにより、前記少なくとも１つの記憶手段の良否をテストするスキャン手段（１５２，１５３）と、

前記スキャン手段が、前記第３の記憶手段をアクセスすることを禁止する禁止手段（図７）と、をさらに備えることを特徴とする請求項１に記載の記憶装置。

【請求項３】前記第１の記憶手段は、書き換え可能な不揮発性メモリから構成され、

前記第２の記憶手段は、前記書き換え可能な不揮発性メモリの一部の領域から構成され、

前記第３の記憶手段と前記第４の記憶手段は、不揮発性メモリから構成されている、

ことを特徴とする請求項１又は２に記載の記憶装置。

【請求項４】前記期待値は、この記憶装置に予め記憶されており、又は、外部から供給された値である、ことを特徴とする請求項１、２又は３に記載の記憶装置。

【請求項５】前記関数は一方向性の関数（ハッシュ関数）である、ことを特徴とする請求項１乃至４のいずれか１項に記載の記憶装置。

【請求項６】前記第３の記憶手段と前記比較手段は、一体に封止され（ＬＳＩ）、前記第３の記憶手段と前記比較手段との通信内容は、外部に出力されないように構成されている、

ことを特徴とする請求項１乃至５のいずれか１項に記載の記憶装置。

【請求項７】機密情報を記憶する機密情報記憶手段（Ｔ２）と、

2

前記機密情報記憶手段をテストするためのテスト情報を記憶したテスト情報記憶手段（Ｔ４）と、

外部より供給される前記機密情報記憶手段のテストを指示する指示信号を受信する受信手段（１５１）と、

前記受信手段により受信された指示信号に応答し、前記テスト情報記憶手段に記憶されたテスト情報により前記機密情報を処理し、処理結果と期待値を比較し、比較結果を出力する出力手段（１５，Ｔ３）と、を備えることを特徴とする記憶装置。

【請求項８】前記テスト情報は、前記機密情報を処理する一方向性の関数（ハッシュ関数）から構成される、ことを特徴とする請求項７に記載の記憶装置。

【請求項９】前記期待値は、この記憶装置に予め記憶されており、又は、外部から供給されて前記受信手段により受信された値である、ことを特徴とする請求項８に記載の記憶装置。

【請求項１０】前記機密情報は、データを暗号化及び／又は復号化するための暗号化された鍵を復号するための情報から構成され、

前記テスト情報は、所定の関数から構成される、ことを特徴とする請求項７、８又は９に記載の記憶装置。

【請求項１１】外部からの直接のアクセスが禁止されており、機密情報を記憶するメモリのテスト方法であって、

前記メモリに記憶されているデータを予め定められた方法で処理し、処理結果と期待値とを比較し、比較結果に基づいて、前記記憶内容の適否を判別する、ことを特徴とするテスト方法。

【請求項１２】外部からの直接のアクセスが禁止されており、暗号化された暗号化鍵を復号するための鍵復号情報を記憶するメモリのテスト方法であって、

前記メモリに記憶されているデータを予め定められた方法で処理し、処理結果と期待値とを比較し、比較結果に基づいて、前記メモリに記憶された前記鍵復号情報の適否を判別する、ことを特徴とするテスト方法。

【請求項１３】前記予め定められた方法は、前記データを一方向性の関数で処理する方法である、ことを特徴とする請求項１１又は１２に記載のテスト方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、記録装置のテスト技術に関し、特に、暗号化鍵、暗号化鍵を復号するための情報、機密文書等の外部に対し秘密の状態に維持したい情報を記憶した記憶装置のテスト技術に関する。

【０００２】

【従来の技術】コンピュータ技術の発展に伴い、機密情報の保護の必要性が増大している。このため、データを暗号化して記憶したり、送信したりする暗号化技術の重要性が高まっており、コンピュータの外部メモリに格納するデータを暗号化して記憶すること等も実施されてい

る。例えば、記憶装置に暗号化鍵を格納しておき、記憶対象データをこの暗号化鍵を用いて暗号化してメモリに格納し、メモリから読み出されたデータを復号化鍵を用いて復号化することが行われている。

【０００３】一方、製品の出荷時等に、記憶媒体の良否をチェックするためには、記憶媒体が正常にデータを記憶し、記憶したデータを出力できることを確認しなければならない。このため、従来は、予め定められたテストパターン等をメモリに記憶させてから、これを読み出して、両者を比較すること等が行われている。また、読み出し専用メモリについては、記憶データを読み出して、読み出したデータと書き込まれているデータとが一致するか否か等を確認している。

【０００４】

【発明が解決しようとする課題】しかし、暗号化鍵を格納したメモリ装置を、この方法でテストすると、暗号化鍵自体が外部に読み出されてしまうという問題があった。

【０００５】この問題を解決するため、メモリの記憶データを変換してから外部に読み出すようにしたテスト機能を備えるメモリ装置も提案されている。しかし、この方法でも、変形されたコードが外部に読み出されるため、変形の方法が推測され、暗号化鍵も推測できてしまうという問題があった。

【０００６】また、特開平８－６３４０２には、ＲＯＭに記憶されたデータと外部から供給する期待値とを比較して、比較結果を出力することにより、ＲＯＭの記憶データを直接外部に読み出すこと無く、ＲＯＭをテストする機能を有する半導体集積回路が提案されている。しかし、この方法でも、アドレス単位等で、機密データが期待値に一致するか否かを知ることができるため、期待値を順次変更しながらテストすることにより、機密データを特定できてしまう。また、アドレス単位で比較動作を行うため、チェックに膨大な時間を要する。

【０００７】この発明は上記実状に鑑みてなされたもので、データを暗号化して記憶する記憶装置において、暗号鍵等の機密性の高いデータを外部に漏らすことなく、かつ、メモリのテストを可能とするテスト方法及びテスト機能を備えた記憶装置を提供することを目的とする。また、この発明は、機密性の高いデータを格納した記憶装置のテストに適したテスト方法及びテスト機能を備えた記憶装置を提供することを目的とする。

【０００８】

【課題を解決するための手段】上記目的を達成するため、この発明の第１の観点にかかる記録装置は、データを記憶するための第１の記憶手段（フラッシュ１１）と、暗号鍵が暗号化されて記憶されている第２の記憶手段（フラッシュ１１）と、前記暗号鍵（ｋ）を復号化するための復号情報が格納された第３の記憶手段（Ｔ２）と、前記第３の記憶手段をテストするための関数を記憶した第４の記憶手段（Ｔ４）と、前記第３の記憶手段に記憶された復号情報を用いて前記暗号鍵を復号化し、外部より供給されるデータを復号化した暗号化鍵を用いて暗号化して、前記第１の記憶手段に書き込む書込手段（１５）と、前記第３の記憶手段に記憶された復号情報を用いて前記暗号鍵を復号化し、復号化された暗号鍵を用いて前記第１の記憶手段から読み出されたデータを復号化して出力する読出手段（１５）と、前記第３の記憶手段に記憶された復号情報を前記第４の記憶手段に記憶された関数で処理し、得られた値と期待値を比較し、比較結果を出力する比較手段と（１５）、を備えることを特徴とする。

【０００９】第３の記憶手段に復号情報が正しく記憶されているか否かをテストするため、第３の記憶手段の記憶データを外部から読めるように構成すると、復号情報が第三者に知られ、暗号化鍵を復号されてしまう虞がある。

【００１０】そこで、この発明では、テスト用の関数を第４の記憶手段に記憶しておき、復号情報を関数で処理し、処理により得られた値と期待値を比較し、比較結果を出力する。復号情報が正しく記憶されていれば、一致を示す比較結果が出力されるはずであり、復号情報を外部に出力することなく、記憶されている１又は複数の暗号化鍵が正しいものであると判別することができる。また、復号情報を関数で処理し、その処理結果と期待値を比較しているので、期待値から復号情報を推測される虞もない。さらに、復号情報を関数で処理した値と期待値とを比較するので、アドレス単位で復号情報と期待値を比較する場合に比して、比較回数を減少させ、処理を高速化することが可能である。

【００１１】第１、第２、第４の記憶手段については、その記憶内容をスキャンすること等により、正常であるか否かをテスト可能とし、第３の記憶手段については、スキャンアクセスを禁止する手段を配置してもよい。この構成においては、第３の記憶手段の記憶内容を直接アクセスして、その記憶データを読み出す行為も禁止され、復号情報の機密が保持される。

【００１２】例えば、前記第１の記憶手段は、書き換え可能な不揮発性メモリから構成され、前記第２の記憶手段は、前記書き換え可能な不揮発性メモリの一部の領域から構成され、前記第３の記憶手段と前記第４の記憶手段は、不揮発性メモリから構成されている。この構成によれば、暗号化鍵を書き換え可能な不揮発性メモリに格納することができる。従って、記憶装置毎に暗号化鍵を異ならせ、一部の記憶装置の暗号化鍵が解読されても、他の記憶装置の暗号化鍵を推測できないように構成することも可能となる。

【００１３】前記期待値は、この記憶装置の、例えば、上記不揮発性メモリに予め記憶されていてもよく、又は、外部から供給するようにしてもよい。

【００１４】前記関数は、例えば、一方向性関数、例えば、ハッシュ関数である。復号情報を一方向性の関数により処理することにより、復号情報から処理結果の値は一義的に定まるが、処理結果から復号情報が多数予想され、復号情報を推測することが困難となる。

【００１５】前記第３の記憶手段と前記比較手段は、樹脂等で一体に封止され、前記第３の記憶手段と前記比較手段との通信内容は、外部に出力されないように構成されることが望ましい。第３の記憶手段のデータライン等を他の記憶手段のデータラインと一体化すると、第３の記憶手段と比較手段との間でデータを授受している際にデータが外部に漏れる可能性がある。しかし、この構成によれば、第３の記憶手段の記憶内容を機密に保持できる。

【００１６】また、この発明の第２の観点にかかる記憶装置は、機密情報を記憶する機密情報記憶手段（Ｔ２）と、前記機密情報記憶手段をテストするためのテスト情報を記憶したテスト情報記憶手段（Ｔ４）と、外部より供給される前記機密情報記憶手段のテストを指示する指示信号を受信する受信手段（１５１）と、前記受信手段により受信された指示信号に応答し、前記テスト情報記憶手段に記憶されたテスト情報により前記機密情報を処理し、処理結果と期待値を比較し、比較結果を出力する出力手段（１５，Ｔ３）と、を備えることを特徴とする。

【００１７】この発明においても、機密情報を外部に直接読み出すことなく、機密情報が正確に機密情報記憶手段に記憶されていることを判別できる。

【００１８】前記期待値は、この記憶装置に予め記憶されている値でもよく、又は、外部から供給された値でもよい。

【００１９】前記機密情報は、例えば、データを暗号化及び／又は復号化するための暗号化された鍵を復号するための情報から構成され、前記テスト情報は、例えば、所定の関数から構成される。

【００２０】関数としては、例えば、ハッシュ関数等の多（関数に代入する値）対１（演算結果）の関係が成立する一方向性の関数が望ましい。なお、複数の機密情報、例えば、秘密鍵ｎと公開鍵ｅを機密情報記憶手段に記憶させても良い。この場合、例えば、$m^e \bmod n = 0$が成立するか否か等の比較結果から、機密情報が正しく記憶されているか否かを判別することができる。なお、ｍは外部から供給された又は内部に予め記憶されていた定数である。

【００２１】また、この発明の第３の観点に関するテスト方法は、外部からの直接のアクセスが禁止されており、機密情報を記憶するメモリのテスト方法であって、前記メモリに記憶されているデータを予め定められた方法で処理し、処理結果と期待値とを比較し、比較結果に基づいて、前記記憶内容の適否を判別する、ことを特徴とする。

【００２２】これらのテスト方法によれば、メモリの記憶データを直接外部に読み出すことなくテストすることができる。しかも、処理後のデータを比較に使用するので、処理量を低減することも可能である。

【００２３】前記機密情報は、例えば、暗号化された暗号化鍵を復号するための鍵復号情報、機密文書等である。

【００２４】また、前記予め定められた方法は、例えば、前記データを一方向性の関数で処理する方法である。

【００２５】

【発明の実施の形態】以下、この発明の実施の形態にかかるテスト機能を備える記憶装置を、フラッシュメモリを例に説明する。

【００２６】図１は、この発明の第１の実施の形態にかかるテスト機能を備えるメモリ装置の構成を示す。図示するように、この記憶装置１０は、フラッシュメモリ１１と、ＳＲＡＭ１２と、第１のＲＯＭ１３と、第２のＲＯＭ１４と、コントローラ１５と、より構成される。

【００２７】フラッシュメモリ１１は、通常知られているように、ブロック消去型の記憶素子であり、複数のメモリセルから構成された複数のブロックを備え、予め消去されたブロックにのみデータの書き込みが可能なメモリである。フラッシュメモリ１１には、データが暗号化されて記憶されている。このデータは、ファイルアロケーションテーブル（ＦＡＴ）、ディレクトリ情報等のデータを含む。特定のアドレスＴ１には、データを暗号化及び復号化するためのデータ鍵ｋが暗号化されて記憶されている。

【００２８】ＳＲＡＭ（スタティックランダムアクセスメモリ）１２は、揮発性の高速メモリであり、フラッシュメモリ１１に記憶されているデータの論理アドレスと該データが記憶されている位置の物理アドレスとの対応関係を記憶するアドレス変換テーブル、フラッシュメモリ１１の書き込み可能なブロック（消去済みのブロック）の番号を記憶する空きブロックテーブル等のデータを記憶する。また、ＳＲＡＭ１２は、コントローラ１５のワークエリアとしても機能し、データを暗号化及び復号化するための暗号化鍵ｋ（復号化されたもの）が一次的に保存される。

【００２９】第１のＲＯＭ（リードオンリメモリ）１３は、不揮発性のメモリであり、コントローラ１５の動作プログラムを記憶する。第２のＲＯＭ１４は、不揮発性のメモリであり、図２（Ｂ）に示すように、暗号化されたデータ鍵ｋを復号化するための復号プログラムを記憶する復号プログラム記憶エリアＴ２と、後述する期待値Ｄを記憶する期待値エリアＴ３と、ハッシュ関数を記憶するハッシュ関数エリアＴ４等を備える。

【００３０】フラッシュメモリ１１，ＳＲＡＭ１２，及

び第１及び第２のＲＯＭ１３、１４には、互いに異なった物理アドレスが割り当てられている。また、第２のＲＯＭ１４の、復号プログラムエリアＴ２、期待値エリアＴ３、ハッシュ関数エリアＴ４は、それぞれＡ１，Ａ２，Ａ３の先頭番地から開始する。

【００３１】コントローラ１５は、ＣＰＵ（中央処理装置）、ＤＳＰ（ディジタルシグナルプロセッサ）等から構成され、第１のＲＯＭ１３のプログラムエリアに格納されたプログラムに従って動作し、（１）フラッシュメモリ１１へのデータの書き込み動作、（２）フラッシュメモリ１１からのデータの読み出し動作、（３）記憶装置１０内のメモリをテストするテスト動作を行う。

【００３２】コントローラ１５は、機能的には、外部のコンピュータ、テスト装置２０等にバス（データバス及びコントロールバス）２１を介して接続されたＩ／Ｏバッファ（インタフェース回路）１５１と、インタフェース回路１５１に接続された制御部１５２と、アドレスカウンタ１５３と、より構成される。

【００３３】アドレスカウンタ１５３は、内部アドレスバスを介してフラッシュメモリ１１，ＳＲＡＭ１２，ＲＯＭ１３、１４のアドレス端子Addに接続されている。また、制御部１５２の制御端子は、内部制御バスを介してフラッシュメモリ１１，ＳＲＡＭ１２，第１及び第２のＲＯＭ１３、１４の制御端子Contに接続されている。さらに、制御部１５２の第１のデータ入出力端子は、データバスを介してフラッシュメモリ１１と第１のＲＯＭ１３のデータ端子Dataに接続され、制御部１５２の第２のデータ入出力端子は、内部データバスを介してＳＲＡＭ１２と第２のＲＯＭ１４のデータ端子Dataに接続されている。

【００３４】また、ＳＲＡＭ１２、第１のＲＯＭ１３、及びコントローラ１５は、樹脂等により一体にモールドされてＬＳＩ化されており、ＳＲＡＭ１２及び第２のＲＯＭ１４から読み出されたデータがＬＳＩの外部に出力されないように構成されている。

【００３５】次に、上記構成の記憶装置１０、コンピュータ２０及びテスト装置３０の動作を説明する。

【００３６】（１）　相互認証動作

この記憶装置１０を使用する場合、先ず、コンピュータ２０と記憶装置１０の間で相互認証を行う。この相互認証時、コンピュータ２０は、例えば、図示せぬ表示画面に「パスワードを入力してください」等のメッセージを表示する。このメッセージに応答して、ユーザがパスワードを入力する。コンピュータ２０のドライバとコントローラ１５の制御部１５２は、このパスワードに基づいて、相互に認証し、相互認証に成功すると、記憶装置１０の使用を許可して、以後のアクセスを許可する。一方、相互認証に失敗すると、記憶装置１０の制御部１５２は、以後のアクセスを禁止する。

【００３７】（２）　書き込み動作

記憶装置１０にデータを書き込む場合、コンピュータ２０は、バス２１を介して記憶装置１０に書込コマンドを出力する。この書込コマンドがＩ／Ｏバッファ１５１にセットされる。制御部１５２は、このコマンドを解読し、データの書き込みの指示であることを判別すると、図３に示す処理を開始する。まず、制御部１５２は、Ｉ／Ｏバッファ１５１を介して、バス２１上に書き込みデータの送信を要求するコマンドを出力する（ステップＳ１）。

【００３８】この要求に応答して、コンピュータ２０は、書き込みデータの総量と、先頭の論理アドレスを送信する。続いて、コンピュータ２０は書き込みデータを順次送信する。

【００３９】制御部１５２は、コンピュータ２０から送信されて来たデータ総量と先頭論理アドレスをＩ／Ｏバッファ１５１を介して取り込む（ステップＳ２）。

【００４０】制御部１５２は、フラッシュメモリ１１をアクセスし、暗号化された暗号化鍵ｋを読み出し、これを第２のＲＯＭ１４の復号プログラムエリアＴ２に格納された復号プログラムで復号して、平文の暗号化鍵ｋを生成し、ＳＲＡＭ１２に格納する（ステップＳ３）。この際、第２のＲＯＭ１４から読み出されたデータ（暗号化された暗号化鍵ｋ）及び復号された暗号化鍵ｋは内部データバスＩＤを介して転送されるため、ＬＳＩの外部からは一切アクセスすることができない。

【００４１】次に、制御部１５２は、フラッシュメモリ１１のブート領域Ｔ１に格納されているＦＡＴ、空きブロックテーブル等を参照し、書き込み対象の空きブロックを特定する（ステップＳ４）。

【００４２】一方、コンピュータ２０は書き込み対象のデータをデータバス２１上に順次出力する。

【００４３】制御部１５２は、コンピュータ２０から供給されるデータを取り込み（ステップＳ５）、取り込んだデータをＳＲＡＭ１２に保持されている暗号化鍵ｋを用いて暗号化する（ステップＳ６）。制御部１５２は、書き込み制御信号を制御バスＣＢ上に出力し、さらに、データバスＤＢ上に暗号化したデータを出力し、さらに、アドレスカウンタ１５３に書き込みアドレスを発生させることにより、暗号化されたデータをフラッシュメモリ１１に書き込む（ステップＳ７）。

【００４４】制御部１５２は、あるアドレスについて書き込みが終了すると、全てのデータについて処理を終了したか否かを判別し（ステップＳ８）、終了していなければ、アドレスカウンタ１５３を更新して（ステップＳ９）、ステップＳ５にリターンして、同様の動作を繰り返す。

【００４５】なお、現在の書込対象ブロックが一杯になった場合には、ステップＳ９で次の空きブロックを選択し、選択した空きブロックのアドレスがアドレスカウンタ１５３にセットされ、データが次の空きブロックに書

き込まれる。

【００４６】制御部１５３は、データを格納し終わると、フラッシュメモリ１１に格納された空きブロックテーブルとＦＡＴ及びディレクトリ情報を更新する。さらに、ＳＲＡＭ１２に記憶された暗号化鍵ｋを消去し（ステップＳ１０）、処理を終了する。

【００４７】（３）　読み出し動作

記憶装置１０からデータを読み出す場合、コンピュータ２０は、バス２１を介して記憶装置１０に読み出しコマンドを出力する。

【００４８】読み出しコマンドがＩ／Ｏバッファ１５１にセットされると、制御部１５２は、このコマンドを解読し、データの読み出しの指示であることを判別し、図４に示す処理を開始する。まず、制御部１５２は、Ｉ／Ｏバッファ１５１を介して、バス２１上に先頭の論理アドレスと読み出し対象データの総量の送信を要求するコマンドを出力する（ステップＳ１１）。

【００４９】この要求に応答し、コンピュータ２０は、読み出し対象データの先頭アドレス（論理アドレス）とデータ総量をバス２１を介してコントローラ１５に通知する。制御部１５２は、Ｉ／Ｏバッファ１５１を介して先頭アドレスとデータ総量を受信する（ステップＳ１２）。

【００５０】制御部１５２は、フラッシュメモリ１１をアクセスし、暗号化された暗号化鍵ｋを読み出し、これを第２のＲＯＭ１４の復号プログラムエリアＴ２に格納された復号プログラムで復号して、平文の暗号化鍵ｋを生成し、ＳＲＡＭ１２に格納する（ステップＳ１３）。この時、第２のＲＯＭ１４から読み出された暗号化された暗号化鍵ｋ及び復号された暗号化鍵ｋは内部データバスＩＤＢを介して転送されるため、ＬＳＩの外部からはアクセスすることができない。

【００５１】次に、制御部１５２は、フラッシュメモリ１１に記憶されているＦＡＴ及びディレクトリ情報から、読出対象ファイルが格納されている物理アドレスを判別し、アドレスカウンタ１５３にセットする（ステップＳ１４）。

【００５２】次に、制御部１５２は、読出制御信号を出力し、アドレスカウンタ１５３が指示する物理アドレスに記憶されたデータを読み出し（ステップＳ１５）、ＳＲＡＭ１２に格納した暗号化鍵ｋを用いて復号化し、復号化したデータをＩ／Ｏバッファ１５１とバス２１を介してコンピュータ２０に送信する（ステップＳ１６）。

【００５３】制御部１５２は、読み出したデータの総量がコンピュータ２０から指示された総量に一致したか否かを判別すること等により、読み出しが終了したか否かを判別する（ステップＳ１７）。読出が終了していない場合には、アドレスカウンタ１５３は、読出アドレス（物理アドレス）を更新する（ステップＳ１８）。以後、同様にして、物理アドレスを順次更新しながら、データを読み出す。指定された量のデータを読み終えたと判断されると、コントローラ１５は読み出し動作を終了する。

【００５４】（４）　テスト動作

テスト動作は、通常は、記憶装置１０の製造時、出荷時等に行われ、記憶装置１０内に配置されているフラッシュメモリ１１とＳＲＡＭ１２については、データを正しく記憶し・読み出せるか否か、ＲＯＭ１３，１４については正しいデータが格納されているか否かをテストする。

【００５５】このテストモードに設定する場合、記憶装置１０は外部のテスト装置３０等に接続され、テスト装置３０はコントローラ１５にテストコマンドを送出する。制御部１５２は、Ｉ／Ｏバッファ１５１を介して提供されたテストコマンドに応答し、まず、図５に示すように、フラッシュメモリ１１をテストするモードに入る。

【００５６】（ａ）フラッシュメモリ１１のテスト

制御部１５２は、フラッシュメモリ１１を一旦初期化する（ステップＳ２１）。続いて、アドレスカウンタ１５３を制御してアドレスを順次更新しながら、記憶データを順次読み出し、Ｉ／Ｏバッファ１５１を介してバス２１上に出力する（ステップＳ２２）。テスト装置２０は、全てのビットが「０」であるか否か、「０」以外のビットが存在する場合には、その物理アドレス等を判別する。

【００５７】全てのデータを読み出すと、制御部１５２は、アドレスを順次更新しながら、全てのビットに値「１」を書き込む（ステップＳ２３）。続いて、アドレスを順次更新しながら、記憶データを読み出し、バス２１上に出力する（ステップＳ２４）。テスト装置２０は全てのビットが「１」であるか否か、「１」以外のビットが存在する場合には、その物理アドレス等を判別する。

【００５８】このようにして、フラッシュメモリ１１については、全てのビットをスキャンして、データの書き込み及び読み出しを繰り返すことにより、その良否のチェックが可能となる。

【００５９】（ｂ）ＳＲＡＭのテスト

フラッシュメモリ１１のテストが完了すると、制御部１５２は、ＳＲＡＭ１２のテストを開始する。まず、制御部１５２は、アドレスカウンタ１５３を制御してアドレスを順次更新しながら、全てのビットに値「１」を書き込む（ステップＳ２５）。続いて、アドレスカウンタ１５３を制御してアドレスを順次更新しながら、ＳＲＡＭ１２の記憶データを読み出し、バス２１上に出力する（ステップＳ２６）。テスト装置２０は全てのビットが「１」であるか否か、「１」以外のビットが存在する場合には、その物理アドレス等を判別する。

【００６０】次に、制御部１５２は、アドレスを順次更

新しながら、全てのビットに値「0」を書き込む（ステップＳ２７）。続いて、アドレスを順次更新しながら、ＳＲＡＭ１２の記憶データを読み出し、バス２１上に出力する（ステップＳ２８）。テスト装置２０は全てのビットが「0」であるか否か、「0」以外のビットが存在する場合には、その物理アドレス等を判別する。このようにして、ＳＲＡＭ１２についても、全てのビットをスキャンしてチェックが可能となる。

【００６１】（ｃ）ＲＯＭ１３、１４のテスト
ＳＲＡＭ１２のテストが完了すると、制御部１５２は、ＲＯＭ１３、１４のテストを開始する。ＲＯＭ１３、１４のテストは、記憶データを読み出し、正しいデータが記憶されているか否かを判別することにより行う。但し、復号プログラムエリアＴ２の記憶データをそのまま読み出すと、復号プログラムが第三者に知られ、暗号化鍵ｋが復号されて、盗用又は悪用される虞がある。そこで、暗号化鍵エリアＴ３については、異なるテスト方法を採用する。

【００６２】まず、制御部１５２は、第１のＲＯＭ１３の先頭アドレスをアドレスカウンタ１５３にセットする（ステップＳ２９）。次に、制御部１５２は、アドレスカウンタ１５３が指示するアドレスが復号プログラムエリアＴ２のアドレス（Ａ１≦アドレス＜Ａ２）であるか否かを判別する（ステップＳ３０）。復号プログラムエリアＴ２のアドレスであると判断された場合、何もせずにアドレスを更新して（ステップＳ３１）、ステップＳ３０にリターンする。

【００６３】一方、復号プログラムエリアＴ２のアドレスではないと判断された場合、そのデータを読み出し（ステップＳ３２）、次のアドレスが存在するか否かを判別し（ステップＳ３３）、存在すれば、アドレスを更新して（ステップＳ３１）、ステップＳ３０にリターンする。このようにして、制御部１５２は、アドレスカウンタ１５３を制御してアドレスを順次更新しながら、第１のＲＯＭ１３の記憶データを順次読み出し、Ｉ／Ｏバッファ１５１を介してバス２１上に出力する（ステップＳ３２）。テスト装置３０は、第１のＲＯＭ１３から読み出したデータが予め定められた値であるか否かを全データについて判別する。即ち、データが正しく記憶されているか否かを判別する。

【００６４】第１のＲＯＭ１３のチェックが完了すると、制御部１５２は、ステップＳ３１で、第２のＲＯＭ１４の先頭アドレス（Ａ１）をアドレスカウンタ１５３にセットする。

【００６５】次に、制御部１５２は、アドレスカウンタ１５３が指示するアドレスが復号プログラムエリアＴ２のアドレス（Ａ１≦アドレス＜Ａ２）であるか否かを判別する（ステップＳ３０）。

【００６６】復号プログラムエリアＴ２のアドレスである場合には、アドレスを更新し（ステップＳ３１）、ステップＳ３０に戻る。従って、復号プログラムエリアＴ２については、データは読み出されない。一方、復号プログラムエリアＴ２のアドレスでない場合には、そのアドレスで指定される位置からデータを読み出し（ステップＳ３２）、バス２１上に出力する。続いて、次のアドレスが存在するか否かを判別し（ステップＳ３３）、存在する場合には、ステップＳ３１に戻ってアドレスを更新した後、前述の動作を繰り返す。

【００６７】テスト装置３０は、提供されるデータが、予め定められている記録パターンと一致するか否か等を判断し、一致しない場合には、そのアドレス等を判別する。

【００６８】ステップＳ３３で、次のアドレスが存在しないと判断された場合には、期待値エリアＴ３及びハッシュ関数エリアＴ４等のデータの読み出しが終了したので、復号プログラムエリアＴ２のテストに移る。

【００６９】まず、制御部１５２は、ハッシュ関数エリアＴ４に記憶されたハッシュ関数Ｈを読み出す（ステップＳ３４）。次に、期待値エリアＴ３に格納された期待値のセットＤｉを読み出す（ステップＳ３５）。制御部１５２は、ハッシュ関数Ｈに、復号プログラムエリアＴ２から順次読み出した所定バイトのデータａ，ｂを代入することにより、ｙｉ＝Ｈ（ａ，ｂ）を求める（ステップＳ３６）。続いて、この値ｙが、期待値Ｄｉに一致するか否かを判別する（ステップＳ３７）。

【００７０】制御回路１５２は、復号プログラムエリアＴ２の全記憶データを読み出すまで、比較動作を繰り返す。例えば、復号プログラムエリアＴ２が４ｋバイトのサイズであり、ａ，ｂがそれぞれ５１２バイトとすれば、４回作業を繰り返す。全ての演算結果と全ての期待値が一致する場合には、一致検出信号をテスト装置２０に送信し（ステップＳ３８）、１回でも不一致の場合には、不一致検出信号をテスト装置２０に送信する（ステップＳ３９）。以上でテスト動作を終了する。

【００７１】このようにして、テスト装置２０は、フラッシュメモリ１１とＳＲＡＭ１２とに関しては、記憶エリアをスキャンしてデータを記憶させて、さらに、これを読み出して、期待値と比較することにより、テストすることができる。復号プログラムエリアＴ２を除く第１、第２のＲＯＭ１３、１４の記憶エリアに関しても、記憶エリアをスキャンして読み出したデータとプログラム自体とを比較することにより、記憶データの適否を判別できる。

【００７２】一方、第２ＲＯＭ１４の復号プログラムエリアＴ２に関しては、その記憶データを直接読み出すことが、ステップＳ３０で禁止されており、記憶データを直接チェックすることはできず、機密情報である復号化プログラムの漏洩を防止できる。しかも、コントローラ１５から供給される比較結果を示すデータから、格納されている復号化プログラムが正しい内容であるか否かを

判別することができる。即ち、演算結果ｙと期待値Ｄが不一致の場合は、何らかの異常がＲＯＭ１３内にあると考えられ、そのチップを排除することができる。即ち、このテスト手法によれば、復号化プログラム等の機密情報を第三者であるテスト実施者に公開することなく、記憶装置１０内のメモリの良・不良を検査することができる。

【００７３】以上説明したメモリテストの機能構成を図６に示す。ここに示すように、ＬＳＩ内の非プロテクトＲＯＭ（外部からアクセスできるＲＯＭ）、即ち、第１のＲＯＭ１３と第２のＲＯＭ１４の復号プログラムエリアを除く部分は、アドレス指定され、その記憶データがＬＳＩの外部に直接読み出され、外部のチェックパターンと比較される。

【００７４】一方、ＬＳＩ内のプロテクトＲＯＭ（外部からアクセスできないＲＯＭ）、即ち、第２のＲＯＭ１４の復号プログラムエリアは、ＬＳＩの外部からアドレス指定され、その記憶データを計算モジュールによって変換する。この内容は、ＲＡＭに格納され、そのＲＡＭの内容から、内部に予め記憶しておいた期待値と比較し、比較結果が外部に出力される。

【００７５】なお、以上の説明では、プロセッサは、Ｄ＝ｙ（＝Ｈ（ａ，ｂ））であるか否かを判別することにより、記憶されている暗号鍵の正当性を判別したが、他の手法を使用することも可能である。

【００７６】例えば、期待値Ｄを公にしておき、テスト装置３０より、期待値Ｄを記憶装置１０に提供するようにしてもよい。この場合は、コントローラ１５は、ハッシュ関数エリアＴ４から読み出した関数Ｈ（）に暗号化鍵ｋを代入して、値を求め、求めた値とコンピュータ本体から提供された期待値Ｄが一致するか否かを判別し、判別結果をテスト装置３０に供給する。

【００７７】なお、関数Ｈは、ハッシュ関数に限定されないが、同一の演算結果に対して複数の変数が対応するものが望ましい。このような構成とすれば、たとえ、期待値Ｄが第三者に知られても、暗号化鍵ｋ自体を特定することはできない。

【００７８】また、暗号化鍵は、複数でもよい。例えば、第２のＲＯＭ１４内に全ての記憶装置１０に共通の暗号化鍵（共通鍵）を記憶させておき、フラッシュメモリ１１にその記憶装置１０に固有の暗号化鍵（固有鍵）を格納してもよい。この固有鍵は、例えば、記憶装置１０を初期化した際に、乱数等に基づいて設定される。さらに、この固有鍵をパスワード等に基づいて暗号化し、暗号化された固有鍵を復号するためのプログラムをフラッシュメモリに格納してもよい。

【００７９】また、暗号化の手法としてＲＳＡ法を使用する場合には、例えば、公開鍵ｅと秘密鍵ｎを使用することができる。この場合、暗号化鍵エリアＴ３のテストには、例えば、ｄ＝m^{e} ｍｏｄ ｎが期待値Ｄに一致するか否かを判別し、判別結果をテスト装置２０に通知するようにしてもよい。この場合、定数ｍは外部から供給してもよく、また、予めメモリに格納しておいてもよい。

【００８０】また、上記説明では、フラッシュメモリ１１及びＳＲＡＭ１２のチェックのために、「１」及び「０」を全ビットに書き込んだが、例えば、所定のテストパターンを書き込んでも良い。また、さらに、複数回「１」又は「０」を書き込んでも良い。

【００８１】また、以上の説明では、テスト装置２０からのテストコマンドに応答して、制御部１５２がアドレスカウンタ１５３を制御して、アドレスを発生して順次データの書き込み及び読み出しを行ったが、テストモードが設定されると、モードが解除されるまでは、外部のバスと内部バスを直結し、外部（テスタ）からの信号により、直接各メモリをアドレッシングし、且つ、制御信号を出力するように制御してもよい。この場合も、例えば、図７に示すように、上位のアドレス信号をデコードする等して、暗号化鍵エリアＴ３がアドレッシングされたときは、ＲＯＭ１３をディスエイブル状態に設定する等、外部からのアドレッシングを受付けない（禁止する）ように、アドレス信号をマスクすることが望ましい。

【００８２】（第２の実施の形態）第１の実施の形態では、フラッシュメモリ１１にデータを書き込んだり、フラッシュメモリ１１からデータを読み出したりする間は、ＳＲＡＭ１２に暗号化鍵ｋが記憶され、暗号化鍵ｋを用いて暗号化及び複合化が行われる。一方、この状態で、動作クロックを停止し、テストモードに入り、ＳＲＡＭ１２の記憶データを読み出すと、暗号化鍵ｋが第三者に知られてしまう虞がある。このため、図８に示すように、テストモードが指示されると、制御部１５２が、ＳＲＡＭ１２に一旦リセット信号を送出して、これをリセットし、その後、外部からの制御に従ったテストを可能としてもよい。

【００８３】以上の説明では、この発明をフラッシュメモリにデータを記憶する際に、データを暗号化及び複合化する暗号化鍵ｋを格納する領域のテストに適用した例を説明した。しかし、この発明は上記実施の形態に限定されない。この発明は、機密性を有するデータを記憶した不揮発性記憶媒体のテストに広く適用可能である。

【００８４】

【発明の効果】以上説明したように、この発明によれば、記憶装置に記憶された機密情報を直接読み出すことなく、機密情報を記憶している領域の良・不良を判別することができる。

【図面の簡単な説明】

【図１】この発明の実施の形態にかかるメモリ装置及びコンピュータ、さらに、テスト装置の基本構成を示すブロック図である。

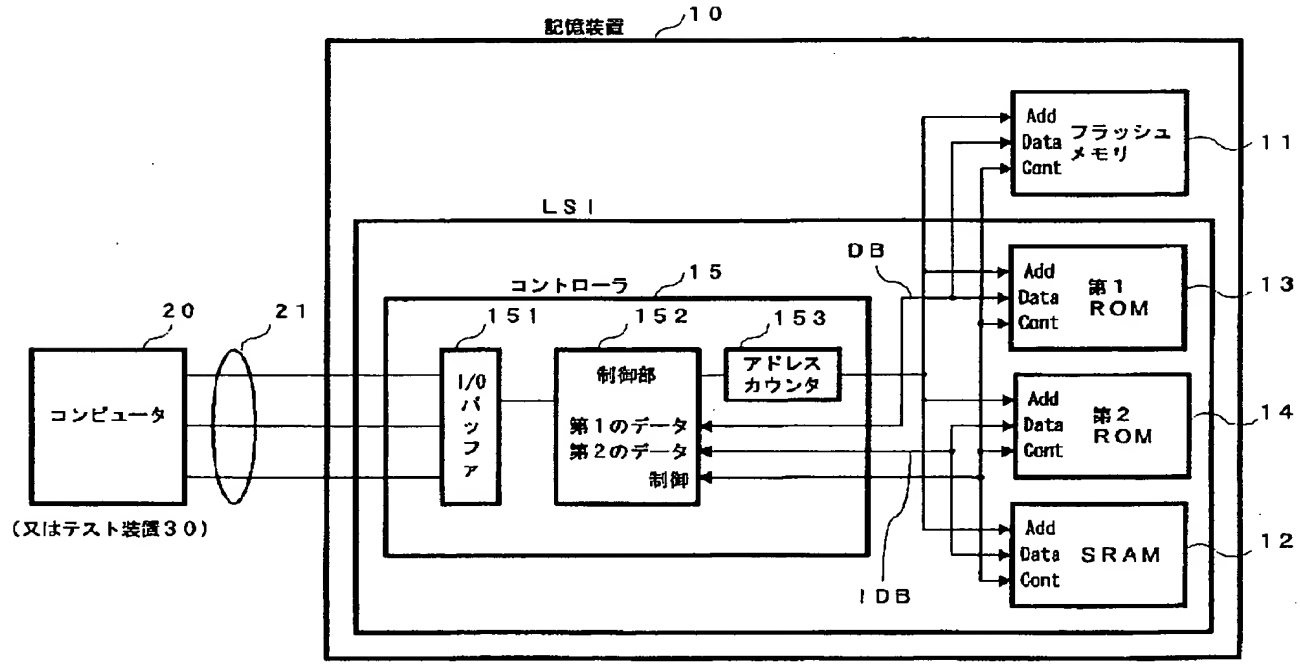
15　　16

【図２】ＲＯＭの内部構成を示す図である。
【図３】フラッシュメモリ１１へのデータ書き込み動作を説明するためのフローチャートである。
【図４】フラッシュメモリ１１からのデータの読み出し動作を説明するためフローチャートである。
【図５】テスト動作を説明するためのフローチャートである。
【図６】テスト動作を説明するための機能ブロック図である。
【図７】機密情報を記憶した領域へのアクセスを禁止する構成の一例を説明するためのブロック図である。
【図８】テストモードで、ＳＲＡＭの内容をリセットする構成の一例を示す図である。

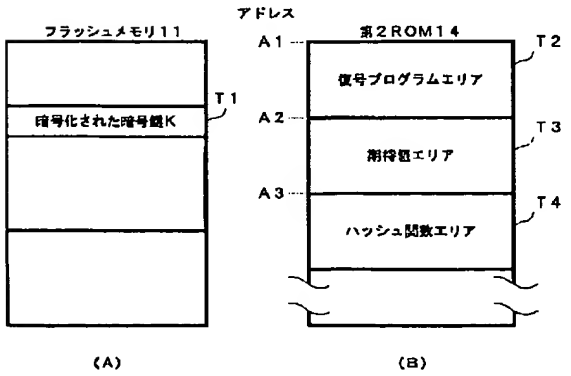
【符号の説明】

１１	フラッシュメモリ
１２	ＳＲＡＭ
１３、１４	ＲＯＭ
１５	コントローラ
２０	コンピュータ
２１	バス
３０	テスト装置
１５１	Ｉ／Ｏバッファ
１５２	制御部
１５３	アドレスカウンタ

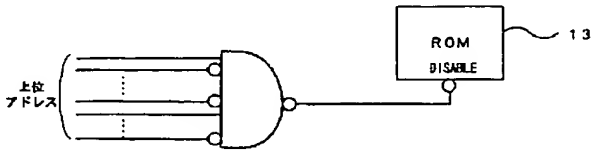
【図１】



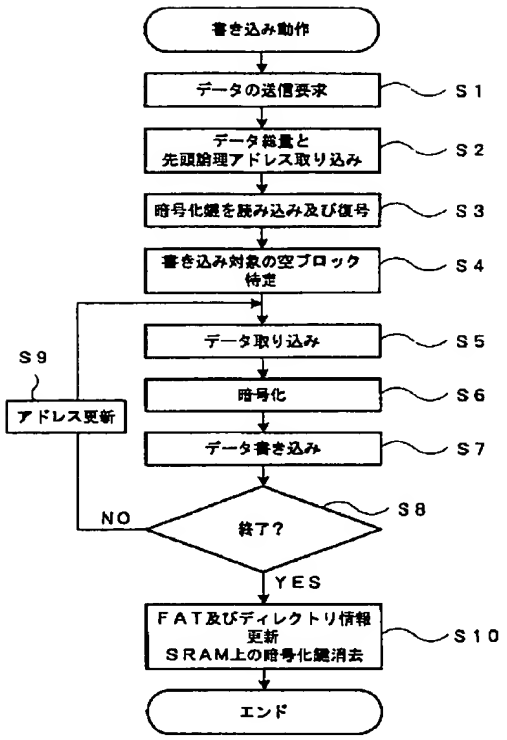
【図２】



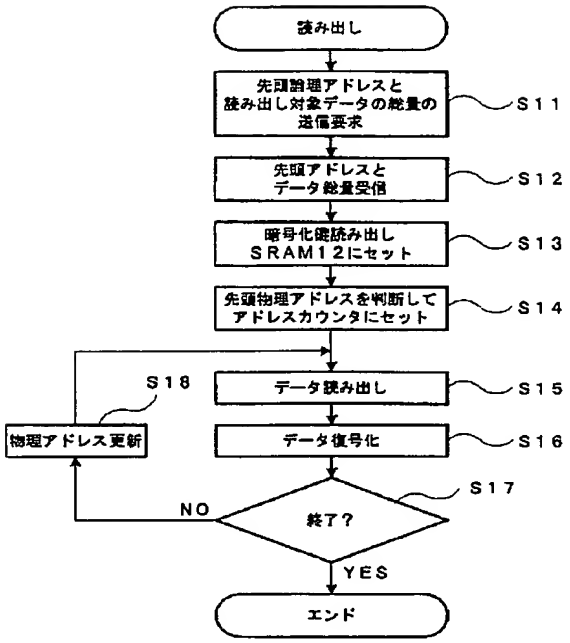
【図７】



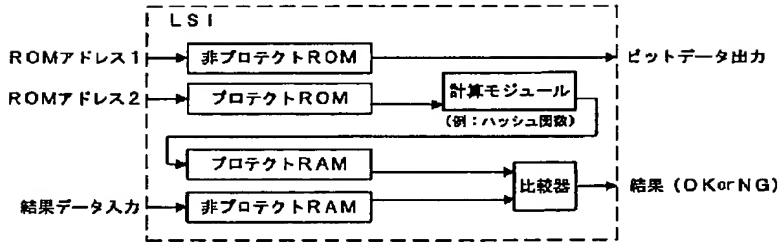
【図３】


書き込み動作
データの送信要求
S１
データ総量と
先頭論理アドレス取り込み
S２
暗号化鍵を読み込み及び復号
S３
書き込み対象の空ブロック
特定
S４
データ取り込み
S５
暗号化
S６
データ書き込み
S７
終了？
S８
NO
YES
S９
アドレス更新
FAT及びディレクトリ情報
更新
SRAM上の暗号化鍵消去
S１０
エンド

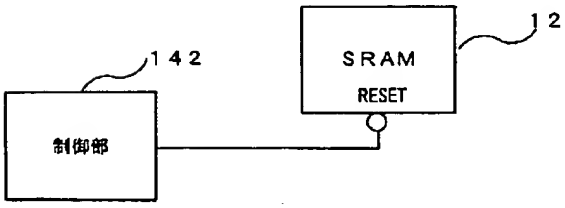
【図４】


読み出し
先頭論理アドレスと
読み出し対象データの総量の
送信要求
S１１
先頭アドレスと
データ総量受信
S１２
暗号化鍵読み出し
SRAM１２にセット
S１３
先頭物理アドレスを判断して
アドレスカウンタにセット
S１４
データ読み出し
S１５
データ復号化
S１６
終了？
S１７
NO
YES
S１８
物理アドレス更新
エンド

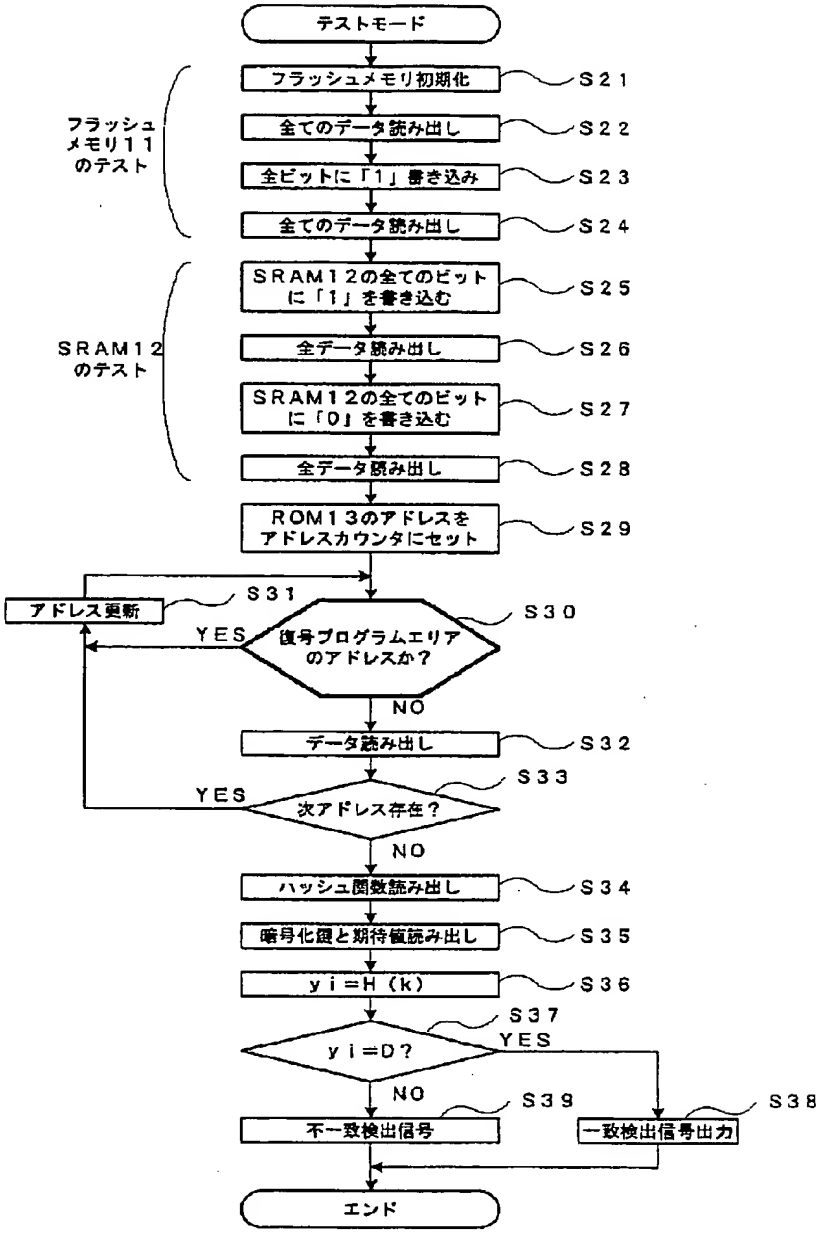
【図６】


LSI
ROMアドレス１
非プロテクトROM
ビットデータ出力
ROMアドレス２
プロテクトROM
計算モジュール
（例：ハッシュ関数）
プロテクトRAM
比較器
結果（OKorNG）
結果データ入力
非プロテクトRAM

【図８】


１２
SRAM
RESET
１４２
制御部

【図５】


テストモード
フラッシュメモリ初期化
S21
全てのデータ読み出し
S22
全ビットに「1」書き込み
S23
全てのデータ読み出し
S24
フラッシュメモリ11のテスト
SRAM12の全てのビットに「1」を書き込む
S25
全データ読み出し
S26
SRAM12の全てのビットに「0」を書き込む
S27
全データ読み出し
S28
SRAM12のテスト
ROM13のアドレスをアドレスカウンタにセット
S29
アドレス更新
S31
YES
復号プログラムエリアのアドレスか？
S30
NO
データ読み出し
S32
YES
次アドレス存在？
S33
NO
ハッシュ関数読み出し
S34
暗号化鍵と期待値読み出し
S35
yi=H（k）
S36
yi=D？
S37
YES
NO
不一致検出信号
S39
一致検出信号出力
S38
エンド